ネットワーク配信における権利保護

Digital Rights Management for Content Delivery over Networks

栃窪　孝也　■ TOCHIKUBO Koya
中島　孝次　■ NAKASHIMA Koji
千々谷　眞英　■ CHIJIYA Masateru

ネットワーク配信における権利保護システムとして，PKIカード（公開鍵暗号を処理可能なICカード）を利用したコンテンツ配信システムを紹介する。PKI（Public Key Infrastructure：公開鍵基盤）は，公開鍵暗号方式を利用したセキュリティインフラであり，インターネットを利用した電子商取引（EC）などで，盗聴，改ざん，なりすましといったリスクを回避する有効な手段として利用されている。提案システムでは，認証や鍵共有などの処理をPKIカード内部で行うことにより，高いセキュリティを実現している。

Toshiba has proposed a content delivery system using public key infrastructure (PKI) cards as an example of a digital rights management system for content delivery over networks. The PKI card is a smart card that can execute the public key cryptosystem. PKI is a security infrastructure using the public key cryptosystem. It is considered an effective way to avoid risks such as unauthorized interception, modification, and fabrication in electronic commerce via the Internet. In the proposed system, security transactions such as authentication and key exchange are carried out within the PKI card. The proposed system therefore provides a highly secure content delivery system.

1　まえがき

インターネット・イントラネットの普及に伴い，映像配信サービスが注目されて久しい。更に近年では，ADSL（Asymmetric Digital Subscriber Line），FTTH（Fiber To The Home），CATV（ケーブルテレビ）に代表されるブロードバンドが普及し，映像や，映像に静止画や文字などを組み合わせたリッチコンテンツの配信サービスが身近なものとなり始めている。

他方，このようなサービスでは，利用者のなりすましや配信コンテンツの盗聴といったオープンネットワーク特有の脅威に加え，利用者の環境は一般にオープンアーキテクチャであるパソコン（PC）のため，利用者自身によるコンテンツの不正コピーといった脅威が存在する。

ここでは，ネットワーク配信の権利保護システムとして，PKIカードを利用したコンテンツ配信システムについて述べる。ここで提案するシステムは，セキュアなコンテンツ配信システムを構築するための基盤技術であり，利用者側でPKIカードを利用することによりシステム全体として高いセキュリティを実現している点が特長である。なお，提案システムで配信されるコンテンツはMPEG-4（Moving Picture Experts Group-phase 4）形式の動画像であり，コンテンツの配信サーバ及びプレーヤはMPEG-4ビデオ配信システムMobileMotion$_{TM}$を利用している。

2　コンテンツのネットワーク配信の脅威

ここでは，動画像デジタルコンテンツのインターネット配信システムを考える。クライアントはPCとし，配信されたコンテンツはPCで閲覧するものとする。このようなシステムでは，以下のような脅威が考えられる（**図1**）。

⑴　なりすましによる不正利用　　サーバとクライアントPCとのデータのやり取りはネットワークを介して行われるため，ネットワークを利用した各種サービスでは，不正利用者による正当な利用者へのなりすましを防ぐ必

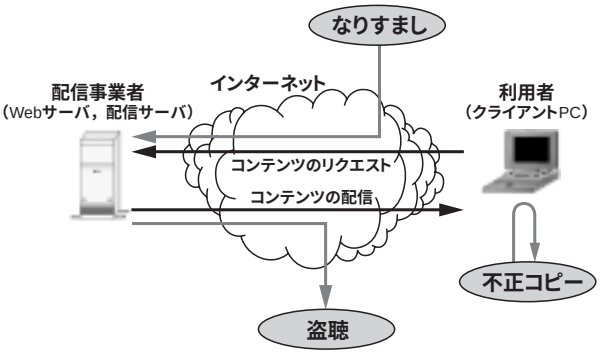

図1．インターネットコンテンツ配信システムの脅威 ― インターネットコンテンツ配信システムには，なりすまし，盗聴，クライアントPCでの不正コピーなどの脅威が存在する。

Risks of content delivery system over the Internet

要がある。特に，課金処理などが必要となってくる有料コンテンツの配信サービスでは，厳密な利用者認証が要求される。

⑵　ネットワーク上のコンテンツの不正利用（盗聴）
　配信されるコンテンツはネットワークを経由してクライアントPCに送られるため，ネットワークの盗聴などからコンテンツを保護する必要がある。

⑶　クライアントPCでの不正コピー　　コピー回数や利用回数などに制限のあるコンテンツは，配信されたコンテンツの（正当な）利用者による不正な利用を防止する必要がある。

また，ネットワークを利用した有料サービスなどでは，利用者情報がネットワークを介してサーバへ送られるため，クライアントのプライバシー保護の観点から，ネットワークを介して送られる利用者情報を保護する必要がある。

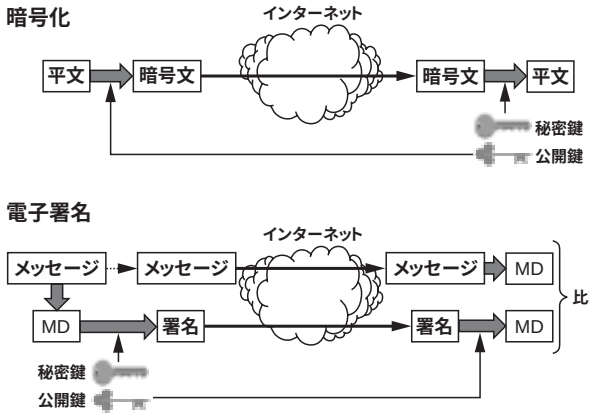

図2．公開鍵暗号方式の概要 ― 公開鍵，秘密鍵の二つの鍵を使って暗号化・復号や電子署名の生成・検証を行う。
Outline of public key cryptosystem

3　PKIの仕組み

PKIは，インターネットを利用した電子商取引などで，盗聴，改ざん，なりすましといったリスクを回避する有効な手段として注目されており，通信データの暗号化と認証を行うプロトコルSSL（Secure Sockets Layer）や暗号・署名メールS/MIME（Secure/Multipurpose Internet Mail Extensions）などに応用されている。

公開鍵暗号方式は，同じ鍵で暗号化・復号を行う共通鍵暗号方式に対し，暗号化と復号で異なる二つの鍵を使用する暗号方式である。あらかじめ秘密鍵，公開鍵と呼ばれる一対の鍵ペアを生成し，公開鍵で暗号化したものは秘密鍵で復号ができ，秘密鍵で署名したものは公開鍵で検証ができるという特長を持っている。秘密鍵は本人だけが保管し，公開鍵は第三者へ公開することで，複数の相手と暗号通信する場合でも管理する鍵は一つでよい。暗号通信する相手の数だけ鍵を管理しなければならない共通鍵暗号方式に比べ，インターネットのようなオープンなインフラに適している。

電子署名は，秘密鍵は本人しか保持していないことを前提に，公開鍵暗号方式の秘密鍵を利用して情報が改ざんされていないことを保証する技術である。送信者がメッセージといっしょに，本人の秘密鍵で送信するメッセージに署名したものを相手に送付する。受信者が送信者の公開鍵で署名を検証して正しければ，送信者以外の第三者によって改ざんされていないことになる。実際の電子署名は，メッセージダイジェスト（MD）を生成する一方向性ハッシュ関数と組み合わせて使用される（**図2**）。

通信相手と暗号通信を行うには相手の公開鍵が必要であるが，インターネット上では通信相手が見えないので，簡単に身分を偽ることができてしまう。本人だと言って送付してきた公開鍵が，ほんとうに本人のものであるという保証はなく，公開鍵の真正性を保証する仕組みが必要である。PKIでは，この保証を信頼できる第三者機関が行い，保証を裏づけるものとして公開鍵の証明書を発行する。発行される証明書を電子証明書（又は，公開鍵証明書）と呼び，信頼できる第三者機関を認証局（又は，認証機関）と呼ぶ。電子証明書を発行する認証局サービスに加入するには，電子証明書を発行してもらうために認証局へ自分の情報と公開鍵を送付し，電子証明書の申請を行う。認証局は，加入者情報の真正性を審査して確かに本人であると確認した場合に，加入者の電子証明書を発行する。電子証明書を発行することで認証局は加入者から信頼され，かつ加入者の公開鍵が認証局に登録されていることを保証する。電子証明書の中には，登録された公開鍵に対応する秘密鍵保持者の情報，登録された公開鍵，証明書を発行した認証局の情報，認証局

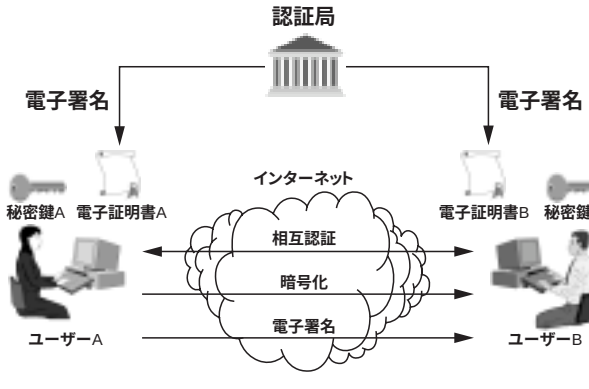

図3．電子証明書と認証局 ― 信頼できる認証局から電子証明書を発行してもらうことで，見えない相手と安全な通信を行うことができる。
Certificate and certification authority

の署名などの情報が含まれている。したがって，電子証明書を入手した者はそれらの情報を得ることができ，認証局の署名を検証することでその証明書が改ざんされていないか（正しい証明書であるか）を確認することができる。

インターネット上で通信をする者は，自分の秘密鍵は厳重に保管して第三者が入手できないようにし，公開鍵は信頼できる認証局に登録する。お互いが信頼できる認証局から発行された電子証明書を入手すれば，見えない相手を確認することができ，正当な者どうしが安全な通信を行うことができる。これを相互認証と呼び，なりすましや否認を防止することができる（**図3**）。

4 PKIカードを利用したコンテンツ配信システム

4.1 システム概要

提案システムでは，ブロードバンドネットワークを利用してコンテンツが配信される。したがって，配信されるコンテンツは，ハイクオリティなものであり，高いセキュリティが要求される。このため，提案システムでは，各利用者にPKIカードを発行し，そのPKIカードを利用者認証やコンテンツ配信に利用することで高いセキュリティを実現している。利用者がサービスを受ける場合，はじめに，クライアントPCからWebサーバに認証のリクエストを送信し，Webサーバ－クライアント間で相互認証を行う。相互認証が正しく行われた場合のみコンテンツの検索を行うことができる。閲覧するコンテンツが決まるとWebサーバから閲覧するコンテンツのコンテンツ情報を取得する。ここまでの操作はクライアントPCのブラウザを使って行われる。

次に，ブラウザが取得したコンテンツ情報をもとにプレーヤが配信サーバに配信リクエストを行い，配信サーバ－クライアントPC間でセッションキーの共有を行う。セッションキーが共有されると配信サーバからコンテンツキー，暗号化コンテンツが配信される。提案システムでは配信されるコンテンツはストリーミング再生のみが可能な仕様となっており，利用者の端末にコンテンツを保存することはできない。なお，このシステムの著作権保護・管理の特長は，以下のとおりである。

⑴ PKIカードを利用した相互認証と鍵共有　　相互認証や鍵共有を行う場合，秘密情報を使う処理はすべてPKIカードの内部で実行する。このため，クライアントPCの不正な解析によるなりすましなどに対しても高いセキュリティを実現している。

⑵ コンテンツ検索情報の保護　　利用者のプライバシー保護の観点から，提案システムでは，利用者情報だけではなくコンテンツ検索処理の際にサーバ－クライアントPC間でやり取りされる情報も暗号化される。

⑶ コンテンツの暗号化配信　　コンテンツは各利用者のPKIカードを使い，配信サーバと共有したセッションキーにより暗号化して配信されるため，ネットワーク上の暗号化されたコンテンツを不正に入手しても，対応するPKIカードを持たないものはコンテンツを正しく復号することができない。

また，このシステムでは，PKIを利用しているため，サーバ側で利用者の秘密情報を保持する必要がない構成になっている（**図4**）。

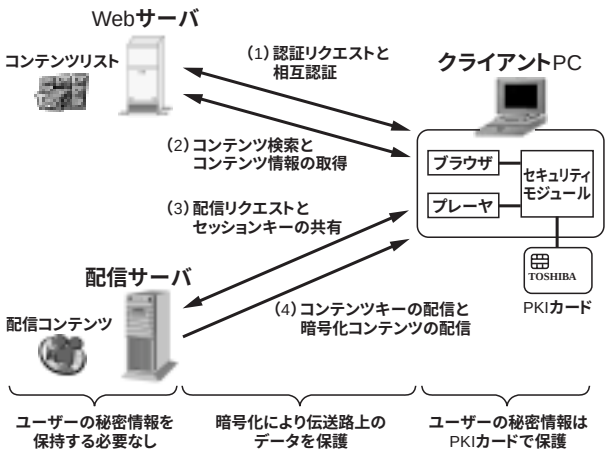

図4．提案システムの構成 ― Webサーバからコンテンツ情報を取得し，配信サーバからコンテンツが配信される。
Components of proposed system

4.2 Webサーバ－クライアントPC間の処理

次に，Webサーバ－クライアントPC間の処理の詳細を述べる。クライアントPCがWebサーバから閲覧するコンテンツのコンテンツ情報を取得するまでの処理手順は，以下のとおりである（**図5**）。

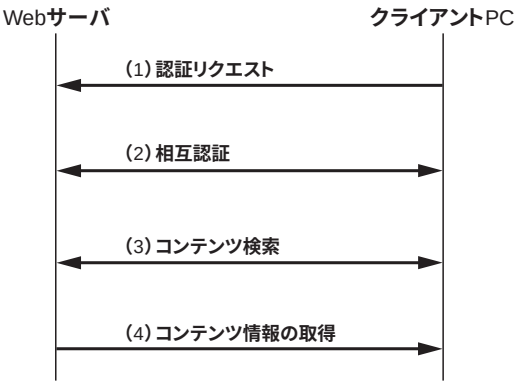

図5．コンテンツ配信の流れ（1） ― 閲覧するコンテンツが決まるとWebサーバから閲覧するコンテンツのコンテンツ情報を取得する。
Flow of content delivery（1）

⑴　クライアントPCは，Webサーバに対し認証リクエストを行う。
⑵　Webサーバは，クライアントPCから認証リクエストがあると，Webサーバの電子証明書をクライアントPCへ送信する。クライアントPCでは送られた電子証明書を検証する（SSLサーバ認証）。Webサーバから送られた電子証明書が正当なものである場合，クライアントPCはWebサーバに自身の電子証明書を送信する。Webサーバ側でも同様に送られた電子証明書を検証する（SSLクライアント認証）。電子証明書の検証が正しく行われなかった場合は，以降の処理は行わない。
⑶　⑵の処理が正常に終了すると，利用者はコンテンツ検索が許可される。提案システムでは，利用者のプライバシ保護の観点から，コンテンツ検索のセッションはSSLにより保護している。
⑷　コンテンツ検索が終了し閲覧するコンテンツが決まると，クライアントPCは，Webサーバから閲覧するコンテンツのコンテンツ情報を取得する。

4.3　配信サーバ－クライアントPC間の処理

次に，配信サーバ－クライアントPC間の処理の詳細を述べる。クライアントPCが，配信サーバから閲覧するコンテンツが配信され，プレーヤで再生するまでの処理手順は以下のとおりである（**図6**）。

⑴　クライアントPCは，取得したコンテンツ情報をもとに配信サーバに配信リクエストを行う。
⑵　配信サーバは，クライアントから配信リクエストがあると，Diffie-Hellman方式により配信サーバ－クライアントPC間でセッションキーを共有する。Diffie-Hellman方式に伴う乱数生成，べき乗剰余演算，電子署名の生成はすべてPKIカード内部で実行される。
⑶　配信サーバは，⑵で共有したセッションキーにより暗号化したコンテンツキーをクライアントPCに送信する。
⑷　配信サーバは，クライアントPCに暗号化されたコンテンツを送信する。暗号化されたコンテンツは，コンテンツのフレームデータ及びフレームキーから構成される。なお，コンテンツは，フレーム単位でフレームキーにより暗号化されており，フレームキーはコンテンツキーにより暗号化されている。

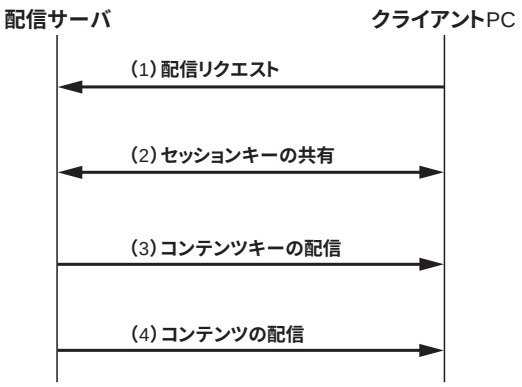

図6．コンテンツ配信の流れ（2） ― セッションキーが共有されると配信サーバからコンテンツキー，暗号化コンテンツが配信される。
Flow of content delivery（2）

5　あとがき

ここでは，ネットワーク配信の権利保護システムとしてPKIカードを利用した著作権保護技術の概要を述べた。ここで述べた権利保護技術は，コンテンツ配信ソリューション／サービスであるDCAMSS™（Digital Content Asset Management Solutions & Services）で利用可能である。DCAMSS™では，映像コンテンツのデータベース化や管理からセキュアなコンテンツ配信までの幅広いASP（Application Service Provider）事業をサポートしている。今後は，DCAMSS™以外の様々な製品にも組み込まれるよう展開を図っていきたい。

文　献

⑴　堀内千尋，ほか．MPEG-4ビデオ配信システムMobileMotion™による応用展開．東芝レビュー．**57**，6，2002，p.38－41.
⑵　能勢健一郎，ほか．PKI構築サービスとPKIカードシステムTARGUSYS™．東芝レビュー．**56**，7，2001，p.34－37.

栃窪　孝也　TOCHIKUBO Koya
e-ソリューション社 SI技術開発センター SI技術担当。暗号・情報セキュリティ技術の研究・開発に従事。電子情報通信学会会員。
Systems Integration Technology Center

中島　孝次　NAKASHIMA Koji
e-ソリューション社 ソリューション第二事業部 ソリューション第二部参事。デジタルコンテンツシステム，MPEG-4システムの開発に従事。
Solutions Div. 2

千々谷　眞英　CHIJIYA Masateru
東芝ITソリューション（株） c-ソリューション事業部。MPEG-4応用システムの開発に従事。
Toshiba IT-Solutions Corp.